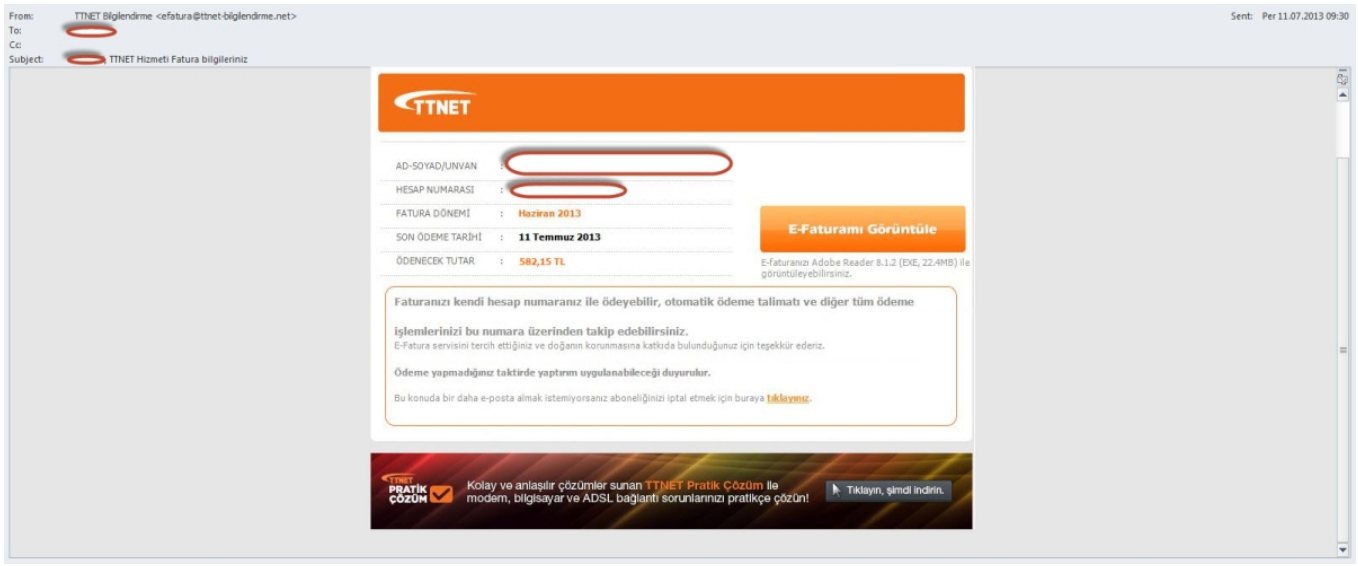
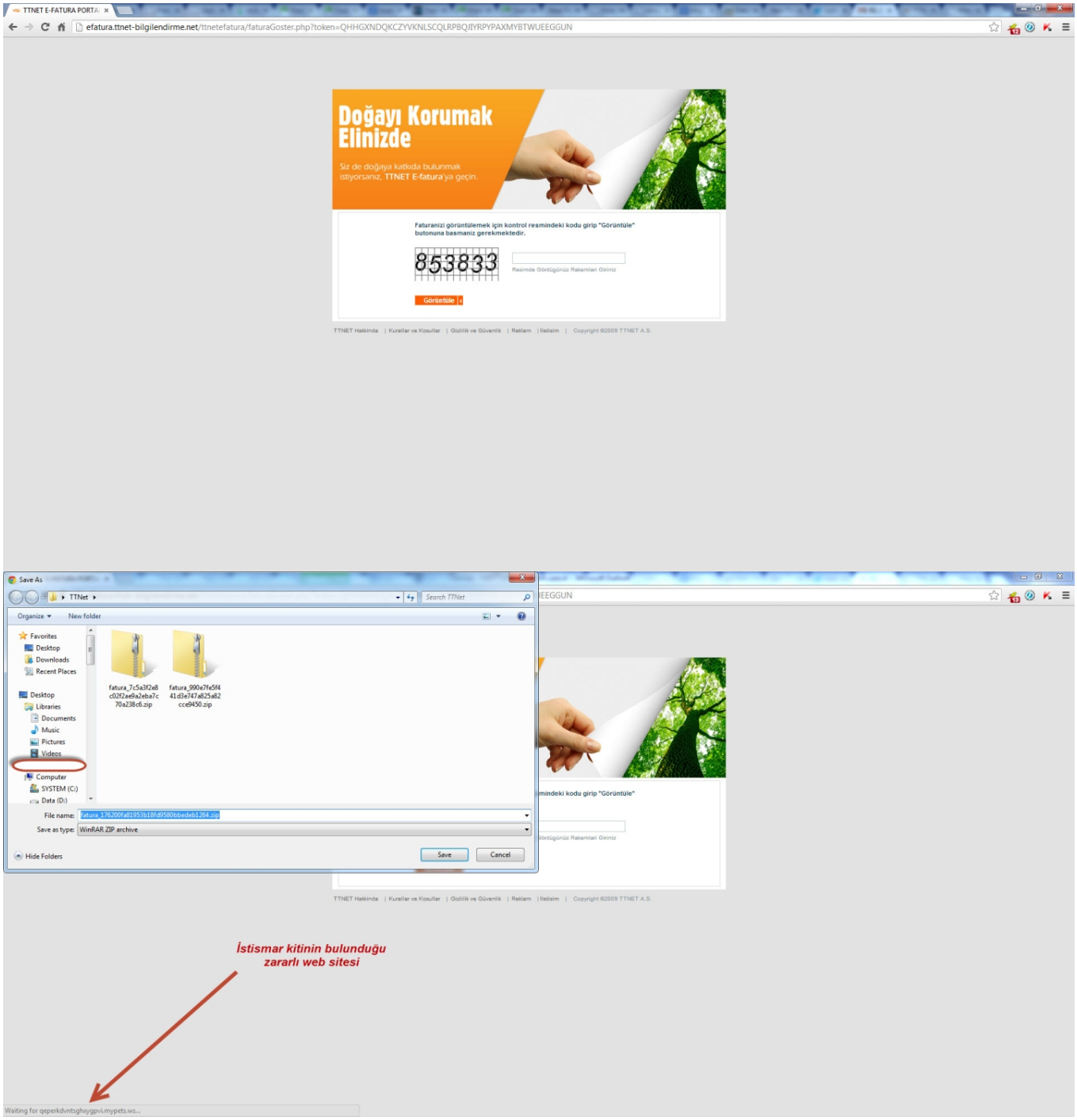
İstismar Kiti Nedir ?

written by Mert SARICA | 1 August 2013

11 Temmuz tarihinde, Aralık ayına damgasını vuran FatMal zararlı yazılımının yenisi ile karşılaştık. Tam olarak yenisi demek belki çok doğru olmayacaktır çünkü bu salgında kullanılan zararlı yazılım ve komuta kontrol merkezinin sürümü bir önceki FatMal komuta kontrol merkezinden farklıydı. Benzer olan tek nokta hemen hemen aynı sahte e-postaların kullanılmış olmasıydı.

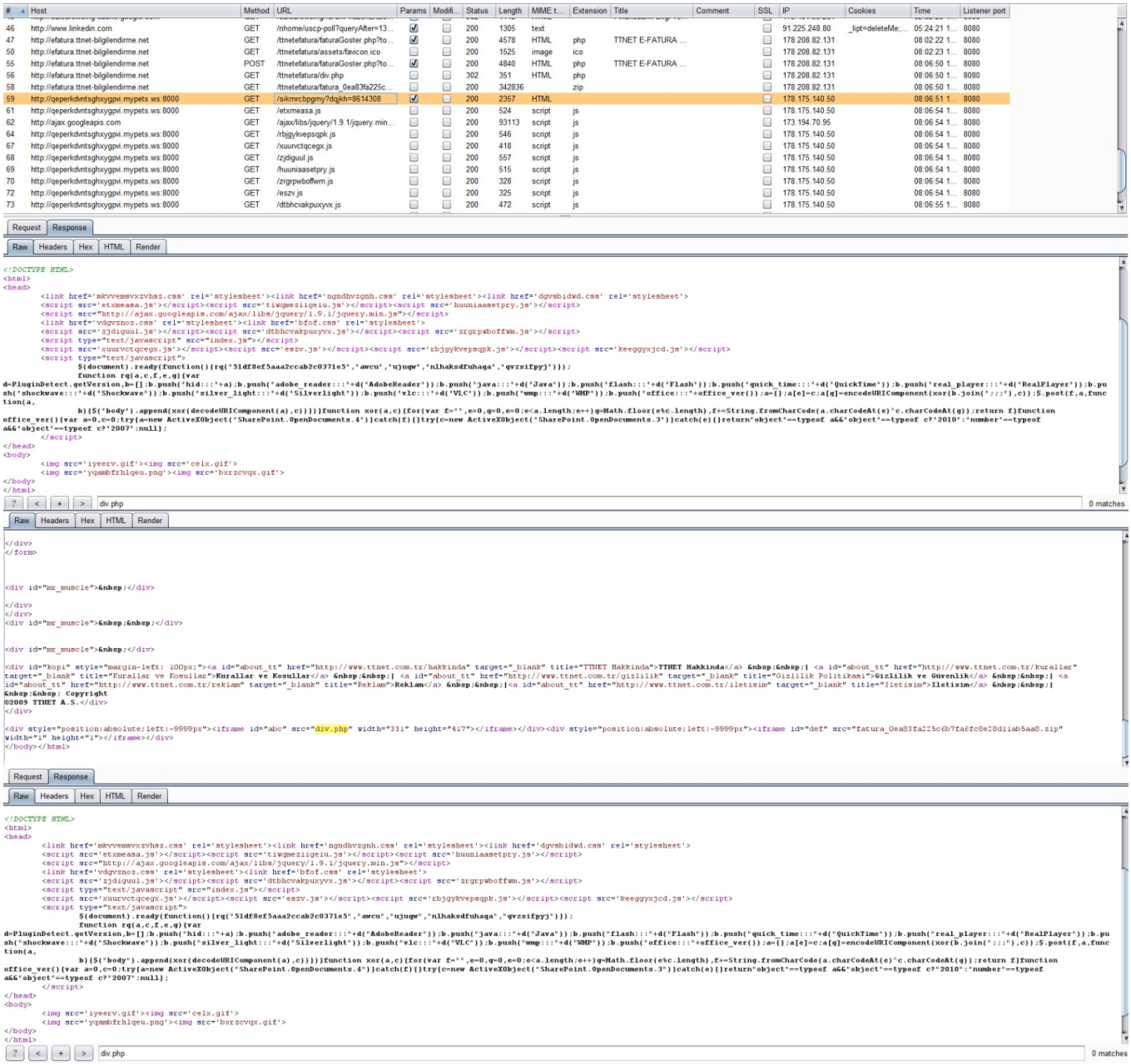


Bu salgın aslında Kasım ayındaki salgında (Hatırlatma: https://internetsube.bddkuyari.com/padm/content/injectus.js) kullanılan zararlı yazılım ve komuta kontrol merkezi sürümü ile neredeyse aynıydı. Bu 3 salgının da arkasında aynı grup mu vardı bilinmez ama bu defa kötü adamlar bir taşla 2 kuş vurmaya çalışmışlardı. Gönderdikleri e-postada yer alan adres ziyaret edildiğinde karşınıza sahte bir fatura görüntüleme sayfası çıkıyordu. Doğru CAPTCHA kodu (inandırıcılık adına her türlü zahmete katlanmışlar :)) girilip GÖRÜNTÜLE butonuna basıldıktan sonra size, adı her defasında değişen ve içinde zararlı yazılım bulunan bir ZIP dosyası gönderiliyordu. Daha önceden dili yananlar, ZIP dosyasını indirip, içinde pdf.exe uzantılı dosyayı gördüğünde bunun zararlı yazılım olduğunu anlayıp, çalıştırmayarak kötü adamların oyununa gelmediklerini düşünerek büyük bir mutluluk ile sahte sayfayı kapatıp, zararlı yazılımı silip işlerine devam ettiler fakat birşeyi gözden kaçırdılar.



GÖRÜNTÜLE butonuna basar basmaz sahte fatura görüntüleme web sitesi, size ZIP dosyasını yollamak ile kalmayıp ayrıca sizi haberiniz olmadan istismar kitinin (Private Exploit Pack olduğunu tahmin ediyorum.) bulunduğu zararlı bir diğer web sitesine de yönlendiriyordu. Siz her ne kadar ZIP dosyasının indirmemiş olsanız da, internet tarayıcınızda bulunan bir zafiyet bu zararlı web sitesi (istismar kitinin yüklü olduğu site) tarafından PluginDetect adındaki javascript kütüphanesi yardımı ile tespit ediliyordu. Ardından istismar kiti yüklü olan bu zararlı web sitesi tarafından zafiyet barındıran internet tarayıcısı eklentilerinize (Java, Adobe PDF Reader, Flash vb.) göre istismar kodu (exploit) gönderilerek sisteminiz ele geçiriliyor (hackleniyor), sisteminize indirmekten ve çalıştırmaktan kaçındığınız o ZIP

dosyası içinde yer alan zararlı yazılım, başka bir yolla sisteminize indirilerek çalıştırılmış oluyordu.



İstismar kitleri son yıllarda bu tür salgınların dışında özellikle Su Kaynağı (Watering Hole) saldırılarında da sıkça kullanılmaktadır. Su kaynağı saldırılarında kötü adamlar, sızmak istedikleri kurumların sistemlerini direkt hedef almak yerine dolaylı yoldan hedef alırlar ve bunun için de hedef kurum tarafından ziyaret edildiği düşünülen web sitelerini hedef olarak seçerler. Örnek ile açıklamak gerekirse mesela birçok çalışan, gün içinde bir defa da olsa takip ettikleri gazetelerin web sitelerini ziyaret ederler. Bunu bilen kötü adamlar da kurum çalışanlarına oltalama saldırısı yapmak yerine sıkça ziyaret edilen gazetelerin web sitelerini hackleyerek, FatMal örneğinde olduğu gibi sayfayı ziyaret edenlerin istismar kiti olan bir diğer zararlı web sitesini ziyaret etmelerini sağlamış olur. Bu sayede bu siteyi ziyaret

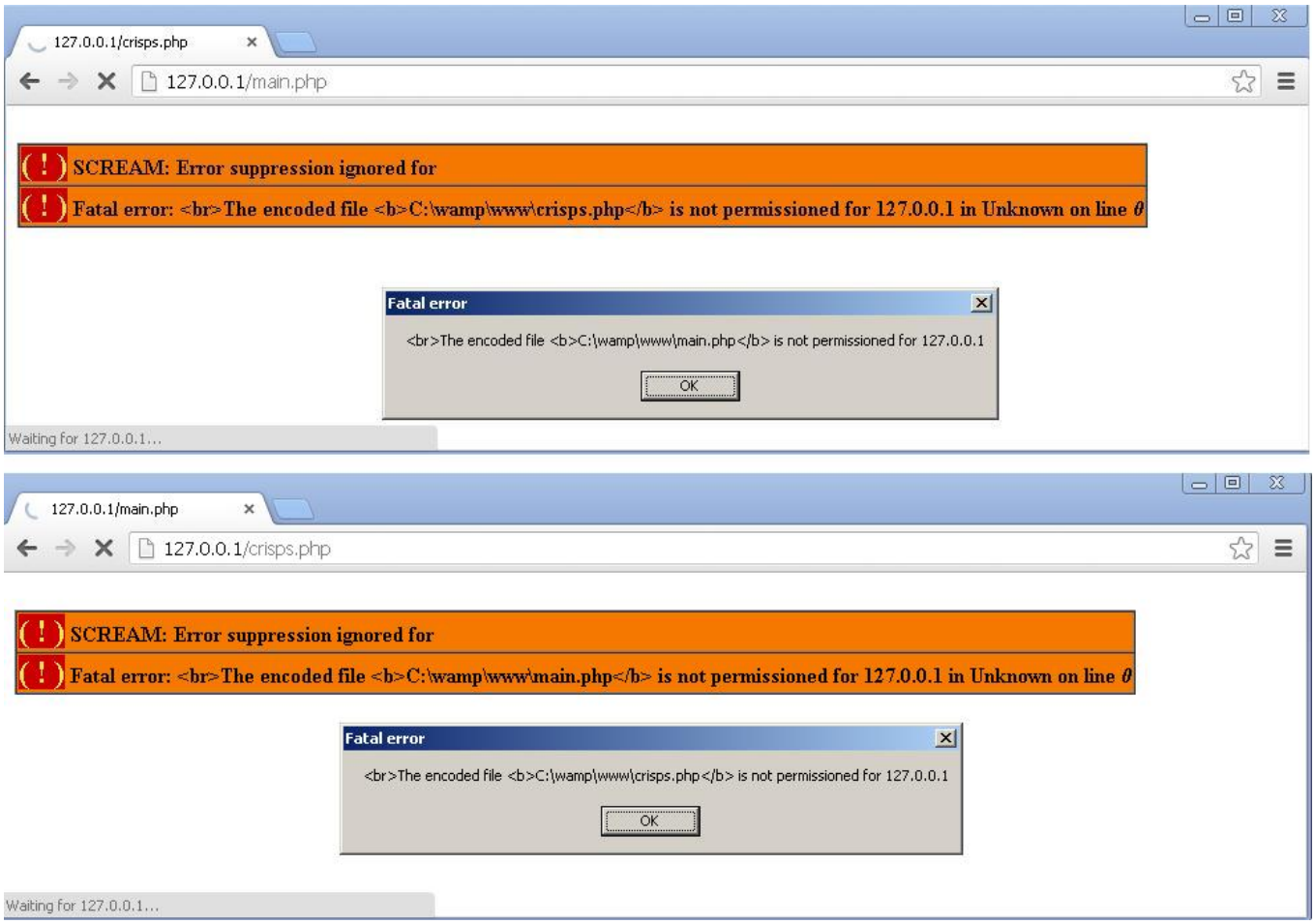
eden yüzlerce farklı kurumun, binlerce kullanıcısının kullanmış olduğu sistemler bu saldırı yöntemi ile bir anda kötü adamların kontrolü altına girmiş olur.

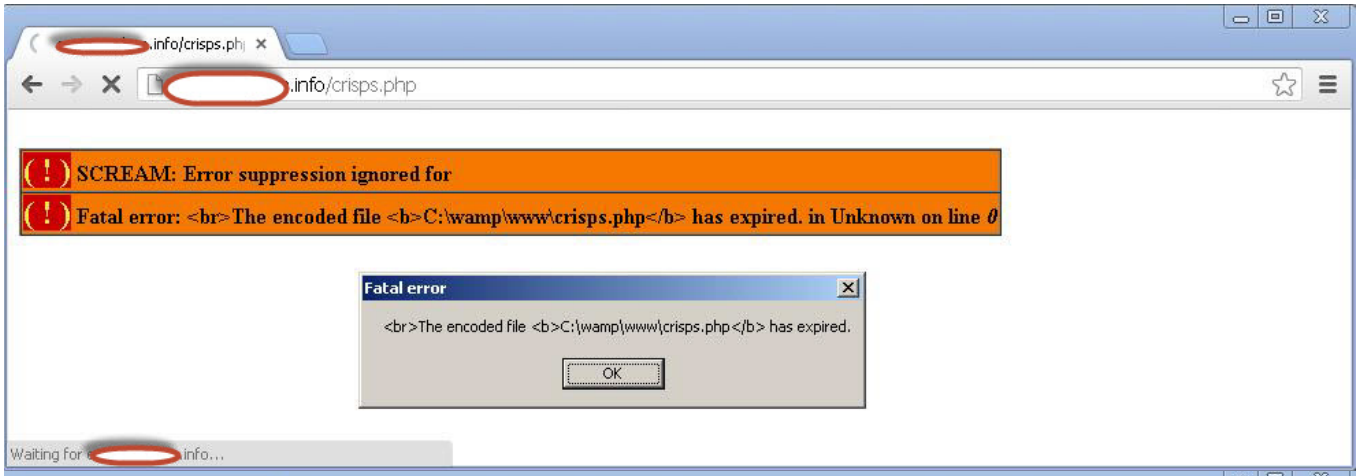
İstismar kiti denilince belki de akla ilk olarak Blackhole istismar kiti gelir. Blackhole istismar kiti aslında onlarca istismar kitinden sadece bir tanesidir fakat onu farklı yapan yeni sürümlerinde çoğunlukla 0. gün istismar kodlarına ev sahipliği yapmasıdır. Metasploit aracına bir uygulamanın istismar kodunun eklenmesinin hemen ardından Blackhole istismar kitine de bu istismar kodunun eklenmesi ve yeni sürümünün geliştiricisi tarafından hızlıca yayınlanması, bu istismar kitinin ne denli tehlikeli olabileceğine güzel bir örnektir.

İstismar kitlerinin oldukça tehlikeli ve siber saldırılarda sıkça kullanılıyor olması nedeniyle zararlı yazılım analistleri, güvenlik uzmanları, emniyet mensupları için bu istismar kitlerinin sanal ortamlara kurulması, analiz edilmesi ve işleyişlerinin anlaşılması, bilgisayar olaylarına müdahale etme açısından oldukça önemlidir fakat çeşitli sitelerden temin edilen bu istismar kitlerinin kullanılması pek o kadar kolay değildir. İstismar kiti geliştiricileri bu işten para kazandıkları için lisanslamaya

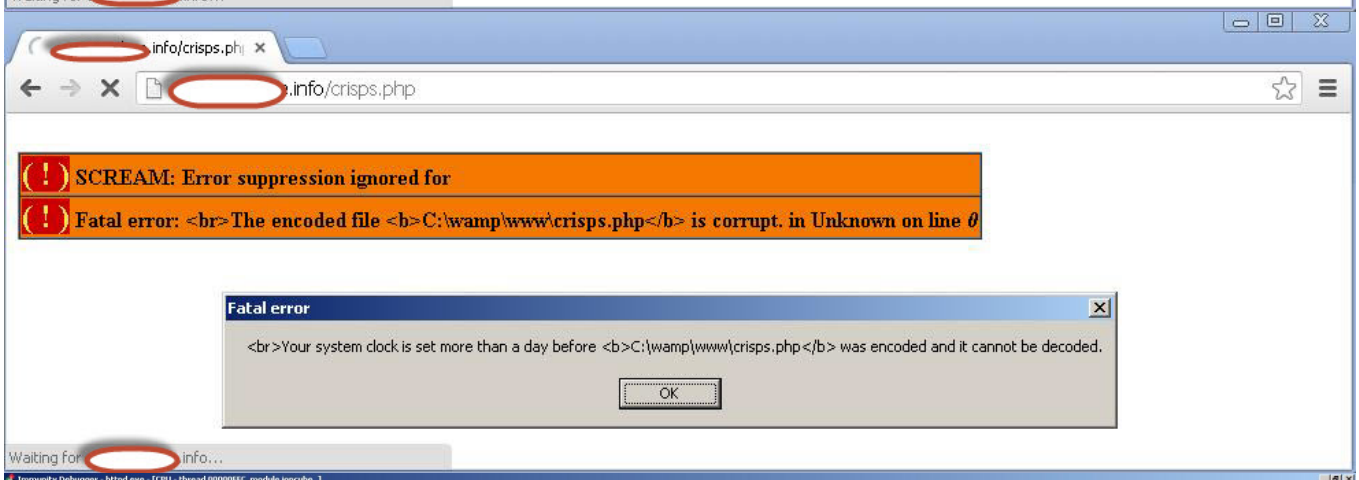
önem vermektedirler dolayısıyla istismar kitlerini kötü adamlara kiralarken veya satarken çeşitli araçlar ile (Örnek: ionCube PHP Encoder) ile istismar kitlerine alan adı bazlı ve zaman bazlı kısıtlamalar koymaktadırlar. Fakat bu kontroller rahatlıkla aşılabildiği için art niyetli kişiler, çeşitli forumlardan temin ettikleri bu istismar kitlerini kurumlara ve kullanıcılara karşı rahatlıkla kullanılabilmektedirler.

Örneğin geçtiğimiz aylarda bir araştırma için sanal makineye Blackhole v2.0.1 istismar kiti kurmam gerektiğinde benim de bu kontrolleri aşmam gerekti. Bunun için öncelikle temin ettiğim Blackhole istismar kitinin hangi internet sitesi için lisanslandığını, bu lisansın hangi tarihe kadar geçerli olduğunu ve bunları kontrol eden fonksiyonları tespit etmem gerekti. Fonksiyonları tespit edip, yamadıktan (patching) sonra sanal makinede bu istismar kitini başarıyla çalıştırabildim.

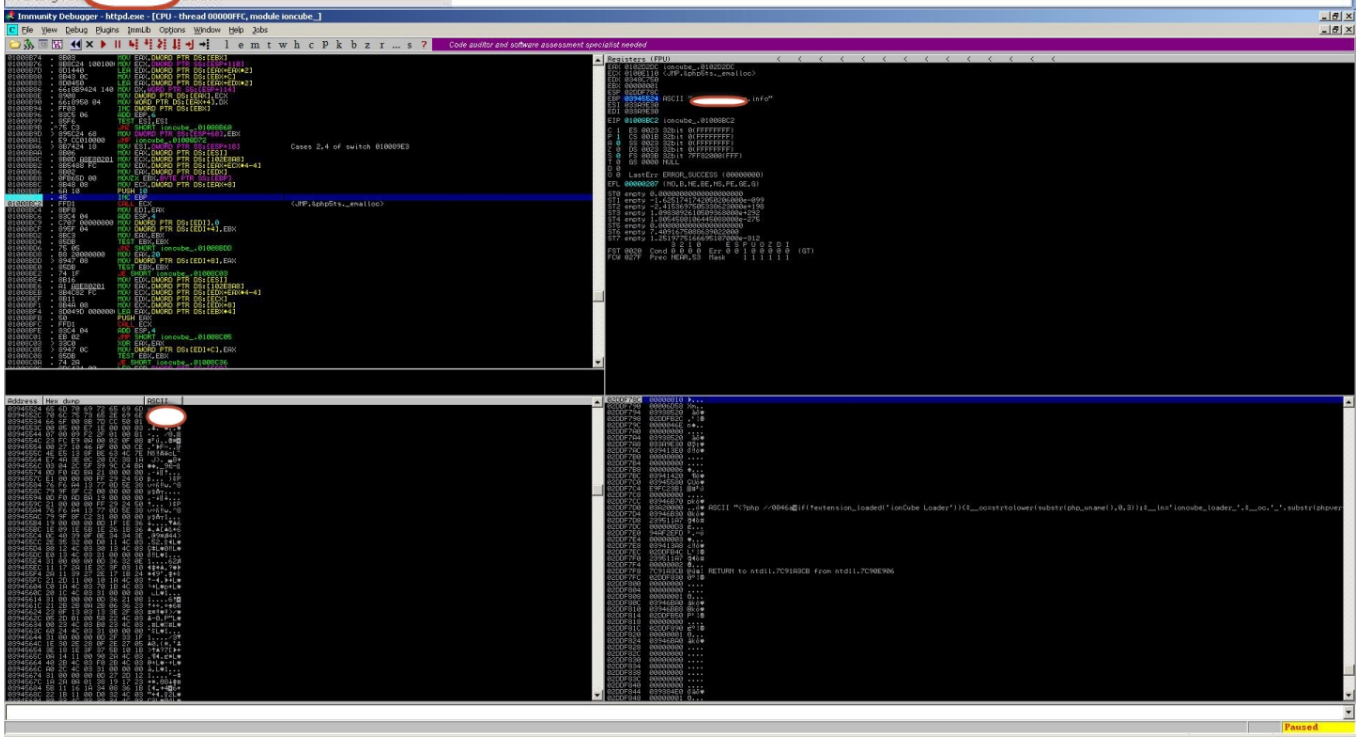


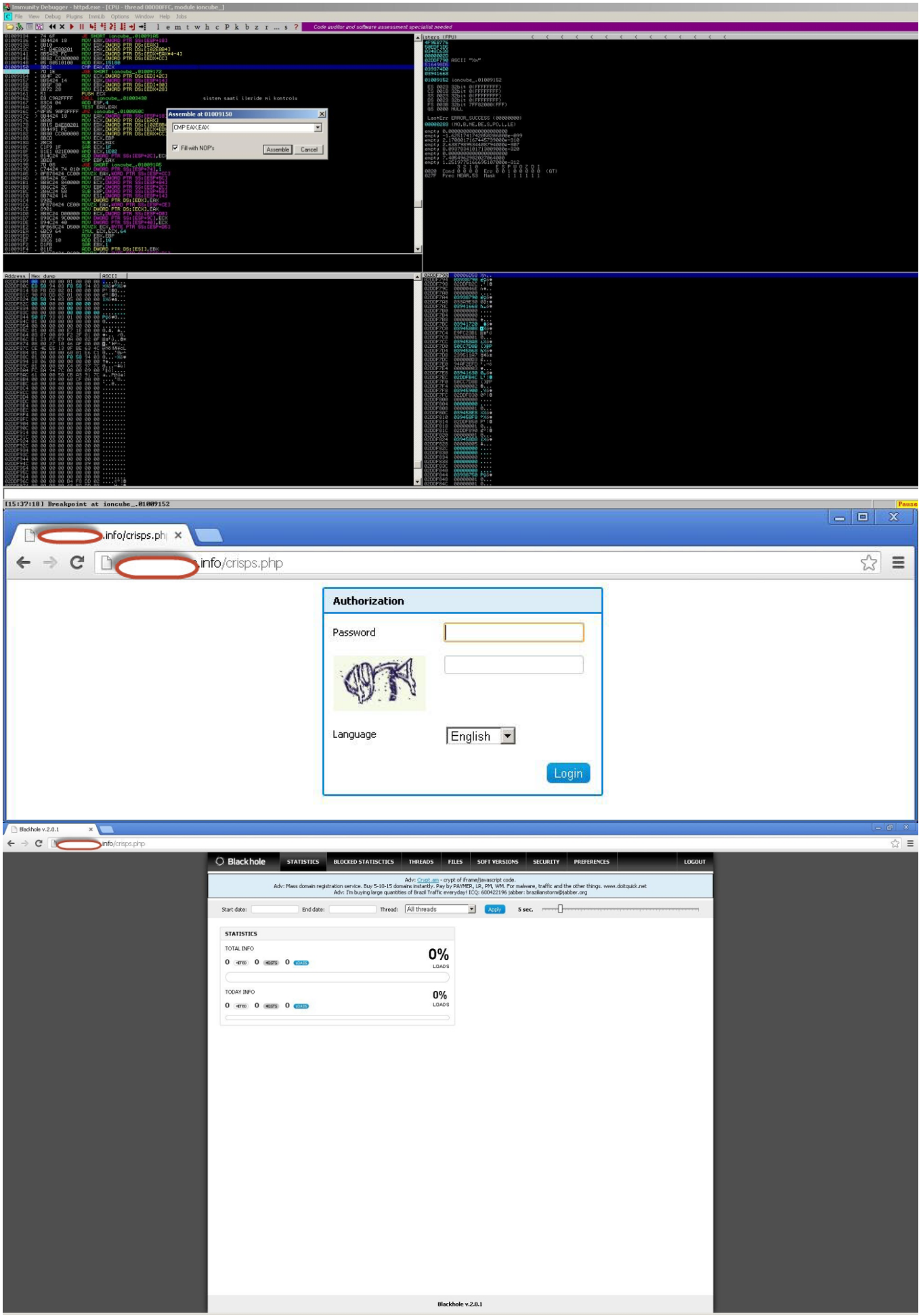

[redacted].info/crisps.php
[redacted].info/crisps.php
SCREAM: Error suppression ignored for
Fatal error:
The encoded file C:\wamp\www\crisps.php has expired. in Unknown on line 0
Fatal error

The encoded file C:\wamp\www\crisps.php has expired.
OK
Waiting for [redacted].info...


[redacted].info/crisps.php
[redacted].info/crisps.php
SCREAM: Error suppression ignored for
Fatal error:
The encoded file C:\wamp\www\crisps.php is corrupt. in Unknown on line 0
Fatal error

Your system clock is set more than a day before C:\wamp\www\crisps.php was encoded and it cannot be decoded.
OK
Waiting for [redacted].info...


Immunity Debugger - httpd.exe - [CPU - thread 00000FFC, module ioncube_]
Paused



Özetle istismar kitleri sıkça güncellendiği, yeri geldiğinde kötü adamlara

kiralanabildiği, forumlardan ücretsiz olarak kolayca temin edilebildiği için kurumlar ve kullanıcıları için büyük bir tehdit haline gelmiştir. Günümüzde kurumlar, sunucularının yama seviyelerine önem verdikleri gibi kullanıcılarının sistemlerinde yüklü olan ve istismar kitleri tarafından istismar edilen Java, Adobe PDF Reader, Flash gibi uygulamaları da yama seviyelerine önem vermeleri gerekmektedir. Son kullanıcıların yani bizlerin ise istismar kitlerinin hedefi olmamaları adına aynı şekilde işletim sistemlerinin ve diğer uygulamaların yama seviyelerini güncel tutmaları, Browser Scan gibi siteler üzerinden yama seviyelerini ara ara kontrol etmeleri ve güvenlik ürünlerinin imzalarını güncel tutmaları gerekmektedir.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.